МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

ИНСТИТУТ ЦИФРОВЫХ ТЕХНОЛОГИЙ, ЭЛЕКТРОНИКИ И ФИЗИКИ (ИЦТЭФ)

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ЭЛЕКТРОНИКИ (ВТиЭ)

**Отчет по лабораторной работе № 3**

по курсу “Защита информация”

**“Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности”**

Выполнил студент 506 гр.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.В. Осипенко

Проверил: ст. преп. кафедры ИБ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.С. Ладыгин.

Лабораторная работа защищена

“\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Цель работы:

В данной работе предполагается продолжение знакомства с документом “Методика оценки угроз безопасности информации”, а также подготовка к созданию модели нарушителя персональной информационной системы.

# Таблица “Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации”:

| **Вид нарушителя** | **Нанесения ущерба физическому лицу** | **Соответствие целей видам риска (ущерба) и возможным негативным последствиям** |
| --- | --- | --- |
| Хакер | Получение финансовой выгоды за счет кражи и продажи персональных данных граждан, желание самореализоваться | У1. (нарушение конфиденциальности персональных данных граждан) |
| Авторизованные пользователи систем и сетей | Непреднамеренные, неосторожные или неквалифицированные действия | У1. (финансовый, иной материальный ущерб физическим лицам) |

# Таблица “Результат определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности”:

| **№ п/п** | **Виды риска (ущерба) и возможные негативные последствия** | **Виды актуального нарушителя** | **Категории нарушителя** | **Уровень возможностей нарушителя** |
| --- | --- | --- | --- | --- |
| 1 | У1:  нарушение конфиденциальности персональных данных граждан;  нарушение личной семейной тайны, утрата чести и доброго имени;  финансовый, иной материальный ущерб физических лиц | Хакер | Внешний | Н3 |
| Авторизованные пользователи систем и сетей | Внутренний | Н2 |

# Таблица “Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности”:

| **№ п/п** | **Вид нарушителя** | **Категория нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| --- | --- | --- | --- | --- | --- |
| 1 | Хакеры (Н2) | Внешний | ПК пользователя;  Локальная сеть и подключенные к ней устройства. | Доступ через локальную вычислительную сеть | Внешнее вредоносное ПО |
| Съемные машинные носители информации, подключенные к ПК | Использование уязвимостей конфигурации системы управления доступом к ПК пользователя |
| 2 | Авторизованные пользователи систем и сетей (Н1) | Внутренний | ПК пользователя | Прямой физический доступ | Ошибочные, неосознанные действия в ходе настройки и использования ПК |

# Вывод:

В ходе данной работы был изучен документом «Методика оценки угроз безопасности информации», и определены источники угроз для моей ИС.

# Контрольные вопросы:

1. С какими видами нарушителей вы встречались в своей практике пользования ИС?

Авторизированные пользователи, Хакеры.

2. Опишите три любых сценария утечки данных из вашей ИС (количество слов в каждом сценарии не менее 50)

- Злоумышленник отправляет вредоносное ПО по электронной почте пользователю локальной сети. Пользователь открывает вложение или нажимает на ссылку, что приводит к заражению компьютера вредоносным ПО. Вредоносное ПО распространяется по локальной сети и подключенным устройствам, шифруя все файлы и данные на своем пути, также собирая конфиденциальные данные, которые оно затем отправляются злоумышленнику.

- Злоумышленник проникает на объект (мою квартиру). Затем с помощью внешнего физического устройства хранения подключается к персональному компьютеру, подключенному к локальной сети. С помощью данного устройства злоумышленник получает физический доступ к серверу локальной сети, содержащему конфиденциальные данные. Он использует данное внешнее физическое устройство хранения для копирования данных на него и выноса их из сети.

- Матушка любит лазить по общедоступной, мировой сети Интернет, при этом не имея каких-либо базовых и продвинутых знаний по Информационной безопасности. И вот, путешествую по различным женским форумам на разные темы и Российским социальным сетям, она может случайно кликнуть на какой-либо баннер, перейти по подозрительной ссылке или скачать небезопасный файл. Вследствие этих действий данные могут быть скомпрометированы или нарушена целостность системы.